UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/435,899	11/08/1999	PAUL JOSEPH SEGER	TU999050	5856

7590 09/10/2004

JOHN H. HOLCOMBE
INTELLECTUAL PROPERTY LAW
8987 E. TANQUE VERDE RD. #309-374
TUCSON, AZ 85749-9610

EXAMINER	
BETIT, JACOB F	

ART UNIT	PAPER NUMBER
2175	

DATE MAILED: 09/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/435,899	SEGER, PAUL JOSEPH	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 19-May-2004, claims 1-50 are presently pending in the application.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 3-5, 17-19, 30-32, and 41-43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3, 17, and 30 recite the limitation "wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key". This limitation renders the claims indefinite because claims 1, 15, and 29, on which they depend, recite the limitation "combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity" which implies that the entire authentication message is combined with the entire user identifier and not just a part of the user identifier as recited in claims 3, 17, and 30. For the purpose of examining it is assumed claims 1, 15, and 29 read --combining the user authentication message

with at least part of the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity--.

Claims 4-5 are rejected because they are dependent on rejected dependent claim 3.

Claims 18-19 are rejected because they are dependent on rejected dependent claim 17.

Claims 31-32 are rejected because they are dependent on rejected dependent claim 30.

Claim 41 recites the limitation "computer processor to conduct said combination by decrypting said user authentication message by said user decrypting key". This limitation renders the claim indefinite because claim 40, on which it depends, recites the limitation "computer processor to combine said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity" which implies that the entire authentication message is combined with the entire user identifier and not just a part of the user identifier as recited in claim 41. For the purpose of examining it is assumed that claim 40 reads -- computer processor to combine said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity--.

Claims 42-43 are rejected because they are dependent on rejected dependent claim 41.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. patent No. 4,9563,769).

As to claim 1, Anderl et al. teaches a portable security system for managing access to a portable data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive (see abstract), the portable security system comprising:

a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive (see page 5, line 31 through page 6, line 23); and

a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface (see figure 1, reference numbers 110, 120, and 130); the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface (see page 5, line 31 through page 6, line 23); the computer processor

receiving the user authentication messages from the data storage drive via the wireless interface, and transmitting the user authorization or denial to the data storage drive via the wireless interface (see page 10, lines 19-26).

Anderl et al. does not teach the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

Smith teaches a security system for computer databases (see abstract), in which he teaches the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 2, lines 11-17), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user (see column 5, lines 9-14 and see figure 1); and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14 and see figure 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. to include the computer processor having a user table comprising at least a unique user identifier for each authorized user and at

least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. by the teachings of Smith because the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity would limit the access of selected users to pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-12).

As to claim 15, Anderl et al. teaches a data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive (see abstract), comprising:

data storage media mounted in the data storage cartridge for storing the data for the read/write access (see figure 1, reference number 115); a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data

storage drive when mounted in the data storage drive (see page 5, line 31 through page 6, line 23); and

a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface (see figure 1, reference numbers 110, 120, and 130); the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface (see page 5, line 31 through page 6, line 23); the computer processor receiving the user authentication messages from the data storage drive via the wireless interface, and transmitting the user authorization or denial to the data storage drive via the wireless interface (see page 10, lines 19-26).

Anderl et al. does not teach the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

Smith teaches the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 2, lines 11-17), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user (see column 5, lines 9-14 and see figure 1); and combining the user authentication message with the user identifier from the user table in

accordance with the predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14 and see figure 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. to include the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. by the teachings of Smith because the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity would limit the access of selected users to pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-12).

As to claim 29, Anderl et al. teaches a method for providing a portable secure interface to a data storage cartridge (see abstract, where it is inherent that "a method for providing a portable secure interface to a data storage cartridge" is disclosed in "a portable data carrier system" that does not provide information of particular applications or file structure to its users), the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive (see figure 1, reference number 115), and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive (see page 5, line 31 through page 6, line 23), the method comprising the steps of:

receiving the user authentication messages from the data storage drive via the wireless interface; and transmitting the user authorization or denial to the data storage drive via the wireless interface (see page 10, lines 19-26).

Anderl et al. does not teach the data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

Smith teaches the data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 2, lines 11-17), the user identifier,

when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user (see column 5, lines 9-14 and see figure 1); and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14 and see figure 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. to include the data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. by the teachings of Smith because the data storage cartridge having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity would limit

the access of selected users to pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-12).

As to claim 40, Anderl et al. teaches a computer program product usable with a programmable Computer processor having computer readable program code embodied therein for providing a secure interface to a data storage cartridge (see abstract), the programmable computer processor mounted in the data storage cartridge (see figure 1, reference number 110), the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive (see figure 1, reference number 115), and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive (see page 5, line 31 through page 6, line 23) , the computer program product comprising:

computer readable program code which causes the programmable computer processor to receive the user authentication messages from the data storage drive via the wireless interface; and computer readable program code which causes the programmable computer processor to transmit the user authorization or denial to the data storage drive via the wireless interface (see page 10, lines 19-26).

Anderl et al. does not teach computer readable program code which causes the programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user

authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combine the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

Smith teaches computer readable program code which causes the programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 2, lines 11-17), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user (see column 5, lines 9-14 and see figure 1); and computer readable program code which causes the programmable computer processor to combine the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity (see column 5, lines 9-14 and see figure 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. to include computer readable program code which causes the programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and computer readable program code which causes the programmable computer processor to combine the user authentication

message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. by the teachings of Smith because computer readable program code which causes the programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and computer readable program code which causes the programmable computer processor to combine the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity would limit the access of selected users to pre-selected locations which they are authorized to access (see Smith, column 1, lines 7-12).

As to claims 6, 20, and 44, Anderl et al. as modified, teaches wherein the computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media (see Smith, column 4, lines 59-66), 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to the user table (see Smith, column 3, line 62 through column 4, line 14).

As to claims 8, 22, and 46, Anderl et al. as modified, teaches wherein the computer processor user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct (see Smith, column 2, lines 11-17).

As to claims 9 and 23, Anderl et al. as modified, teaches wherein the computer processor additionally comprises a nonvolatile memory storing the user table (see Anderl et al., page 11, lines 21-26).

As to claim 33, Anderl et al. as modified, teaches wherein the user table comprises a plurality of the permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media (see Smith column 4, lines 59-66), 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to the user table; and wherein the transmitting step comprises transmitting authorization to conduct the selected the user permitted activities the user is authorized to conduct (see Smith, column 3, line 62 through column 4, line 14).

As to claim 35, Anderl et al. as modified, teaches wherein the step of providing the user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted activities from the user separate entry (see Smith, column 2, lines 11-17).

6. Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44, and 46 above, and further in view of Davis (U.S. patent No. 4,941,201).

As to claims 2 and 16, Anderl et al. as modified, does not teach wherein the wireless interface comprises an RF interface.

Davis teaches an electronic data storage apparatus (see abstract), in which he teaches wherein the wireless interface comprises an RF interface (see column 5, lines 55-61 and see column 21, lines 31-46, where 100 kHz is in the RF range of the Electromagnetic Spectrum).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein the wireless interface comprises an RF interface.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Davis because wherein the wireless interface comprises an RF interface would make the propagation delay between the outputs of the inverters 5 microseconds (see Davis, column 21, lines 39-46).

7. Claims 3-5, 17-19, 30-31, and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S.

patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44, and 46 above, and further in view of Wright et al. (U.S. patent No. 6,084,969).

As to claims 3, 17, 30, and 41, Anderl et al. as modified, does not teach wherein each the user identifier comprises a user symbol and a user decrypting key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key.

Wright et al. teaches an encryption system for a two way pager (see abstract), in which he teaches wherein each the user identifier comprises a user symbol and a user decrypting key (see column 11, line 65 through column 12, line 5), wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key (see column 12, lines 5-13).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein each the user identifier comprises a user symbol and a user decrypting key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Wright et al.

because wherein each the user identifier comprises a user symbol and a user decrypting key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key would authenticate the sender and protect the contents of the message (see Wright et al., column 9, lines 51-56).

As to claims 4, 18, 31, and 42, Anderl et al. as modified, teaches wherein the user decrypting key comprises a sender public key, and wherein the predetermined algorithm comprises a public key cryptographic algorithm (see Wright et al., column 12, lines 5-13).

As to claims 5 and 19, Anderl et al. as modified, teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key (see Wright et al., column 9, lines 51-56), and wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user (see Wright et al., column 12, lines 5-13).

As to claims 32 and 43, Anderl et al. as modified, teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key (see Wright et al., column 9, lines 51-56), wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, and wherein the combining

step comprises decrypting the user authentication message by the receiver private key and the sender public key, whereby the user authentication message is known to have come from the user (see Wright et al., column 12, lines 5-13).

8. Claims 7, 10-13, 21, 24-27, 34, 36-38, 45, and 47-49 rejected under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44, and 46 above, and further in view of Bapat et al. (U.S. patent No. 6,038,563).

As to claims 7, 21, and 45, Anderl et al. as modified, does not teach wherein the computer processor user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct.

Bapat et al. teaches access control to a database using a permissions table (see abstract), in which he teaches wherein the computer processor user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein the computer processor user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Bapat et al. because wherein the computer processor user table comprises a separate entry for each the user

identifier and the permitted activity the user is authorized to conduct would give a way to grant or deny access to certain users (see Bapat et al., column 11, lines 4-7).

As to claims 10, 24, 36, and 47, Anderl et al. as modified, teaches receiving the user authentication messages from the data storage drive via the wireless interface, and transmitting the class authorization or denial to the data storage drive via the wireless interface (see Anderl et al. page 12, lines 7-15, and see figure 7).

Anderl et al. as modified, does not teach wherein the computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity the class of users is authorized to conduct with respect to the data storage media, the class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user; and wherein the computer processor additionally, upon receiving the user authentication messages, combining the user authentication message with the class identifier from the class table in accordance with the predetermined algorithm to authorize or deny the class activity to the user, and transmitting the class authorization or denial.

Bapat et al. teaches wherein the computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity the class of users is authorized to conduct with respect to the data storage media, the class identifier (see column 10, lines 35-47), when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user (see figure 5); and wherein the computer processor

additionally, upon receiving the user authentication messages, combining the user authentication message with the class identifier from the class table in accordance with the predetermined algorithm to authorize or deny the class activity to the user, and transmitting the class authorization or denial (see figure 6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein the computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity the class of users is authorized to conduct with respect to the data storage media, the class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user; and wherein the computer processor additionally, upon receiving the user authentication messages, combining the user authentication message with the class identifier from the class table in accordance with the predetermined algorithm to authorize or deny the class activity to the user, and transmitting the class authorization or denial.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Bapat et al. because wherein the computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity the class of users is authorized to conduct with respect to the data storage media, the class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user; and wherein the computer

processor additionally, upon receiving the user authentication messages, combining the user authentication message with the class identifier from the class table in accordance with the predetermined algorithm to authorize or deny the class activity to the user, and transmitting the class authorization or denial would make an easy way to define a set of access rules to grant access rights to a broad group of users (see Bapat et al., column 11, lines 56-59) and would help to reduce the amount of data required to define access rules (see Bapat et al., column 9, lines 48-50).

As to claims 11, 25, 37, and 48, Anderl et al. as modified, teaches wherein the computer processor user table additionally comprises any class membership of each the user (see Bapat et al., Column 10, lines 4-10), wherein the user may be authorized with respect to the class table either by the class authorization or by the user authorization (see Bapat et al., figure 15A).

As to claims 12, 26, and 49, Anderl et al. as modified, teaches wherein the computer processor user table and the class table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table (see Bapat et al., column 10, lines 35-47).

As to claims 13 and 27, Anderl et al. as modified, teaches wherein the computer processor additionally comprises a 'nonvolatile memory storing the user table (see Anderl et al., page 11, lines 14-26) and the class table (see Bapat et al., column 7, lines 18-24).

As to claim 34, Anderl et al. as modified, does not teach wherein the user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted activities from the separate entries.

Bapat et al. teaches wherein the user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted activities from the separate entries (see column 10, lines 35-47).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein the user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted activities from the separate entries.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Bapat et al. because wherein the user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct; and wherein the transmitting step

additionally comprises identifying the user permitted activities from the separate entries would give a way to grant or deny access to certain users (see Bapat et al., column 11, lines 4-7).

As to claim 38, Anderl et al. as modified, teaches wherein the user table and the class table comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table; and wherein the transmitting step comprises transmitting authorization to conduct the selected the user and the class permitted activities the user is authorized to conduct (see Bapat et al., column 10, lines 35-47).

9. Claims 14, 28, 39, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. (International Publication No. 87/07062) in view of Smith (U.S. patent No. 4,9563,769) as applied to claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44, and 46 above, and further in view of Hastings et al. (U.S. patent No. 6,370,629 B1).

As to claims 14, 28, 39, and 50 Anderl et al. as modified, teaches wherein the computer processor user table permitted activities comprise at least 1) read access to data stored in the data storage media (see Smith, column 4, lines 59-66).

Anderl et al. as modified, does not teach wherein the data stored in the data storage media is encrypted, and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data.

Hastings et al. teaches giving access to information based on time and geographic position (see abstract), in which he teaches wherein the data stored in the data storage media is encrypted (see column 3, line 63 through column 4, line 4), and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data (see column 5, lines 52-61).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, to include wherein the data stored in the data storage media is encrypted, and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Anderl et al. as modified, by the teachings of Hastings et al. because wherein the data stored in the data storage media is encrypted, and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data would keep an unauthorized user from accessing the files (see Hastings et al., column 5, lines 52-61).

Response to Arguments

10. Applicant's arguments filed on 19-May-2004 with respect to rejected claims have been considered but are moot in view of the new grounds of rejection.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. patent No. 6,477,653 B2 to Naito for teaching an information storage system that only grants access to users that first have access to a different medium (see abstract).

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
1 Sep 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100